REMARKS

In response to the Official Action of January 23, 2007, claims 1-23 and 25-27 have been amended and claims 28-31 are newly submitted. No new matter is submitted.

Claim Objection

Referring now to the formal objections, claims 1-27 are objected to for including numbers and symbols in parenthetical portions of the claims. Those parenthetical portions have been deleted from the amended claims and therefore this objection is believed to be overcome.

Claims 25-27 are objected to under 37 CFR §1.75(c) as being of improper dependent form for failing to further limit the subject matter of a previous claim. Claims 25 and 26 have been amended to be in independent form and as such, the claims are believed to be proper.

Referring now to paragraph 5, claims 25 and 27 are stated as failing to further limit method claim 1 and that "a delagator" or "a server" recited in these claims fail to include every feature that they depend on and therefore are improper. Claims 25-27 have been amended to be directed generally to a "delagator/delagatee/server configured to" perform recited operations as fully explained in the specification and shown in Figures 1-3. Consequently, the objection of paragraph 5 is believed to be overcome.

Claim Rejection – 35 USC §101

Referring now to paragraph 6, claims 1-27 are rejected under 35 USC §101 as directed to non-statutory subject matter. Specifically, it is stated that the claim language does not disclose any tangible, useful result such as enabling the use of specific resources after successful authorization. Applicant respectfully disagrees.

Specifically, claim 1 has been amended to specifically point out that resources are accessible via messages on which a secret key operation was applied with said secret master key and wherein said master device is acting as a delagator of an authorization to use said specific resources. Claim 1 further recites forwarding a piece of information to a slave device acting as a delagatee of said authorization, which piece of information enables said slave device to perform a partial secret key operation on messages based on said first part of said secret master key and further forwarding said second part of said secret master key to a server for enabling said server to perform a partial secret key operation on messages received from said slave device based on said second part of said secret master key. It is therefore believed that there is a tangible useful result; namely, the achieved shared or delegated authorization. That is, a user (or different users) may now use either the first device (master device, by itself) or the second device (slave device, in cooperation with the server) whenever wishing to access certain resources. This is believed to be very useful and also to be tangible, for example, because information is generated and transmitted between different devices/server.

Furthermore, claim 1 presents the operations performed by the master device. The master device itself does not need making use of the forwarded information for accessing resources. Thus, from the master device point of view, all required operations are in fact included in claim 1.

In short, claim 1 is believed to be statutory because it does enable the slave device to perform a partial secret key operation on messages based on said first part of said secret master key and similarly, provides that a second secret part of said secret master key is forwarded to a server for enabling the server to perform a partial secret key operation on messages received from the slave device based on the second part of said secret master key. It further provides that the messages provide for resources that are accessible if said messages have had a secret key operation applied thereto with said secret master key. Thus, the method sets forth the actions to perform such partial secret key operation on messages by both the slave device and the server based upon the forwarded first part and second part of a secret master key from the master device. Such transferal of information to allow

other devices to apply operations to a message so that the message allows for accessibility to resources by such devices is certainly a tangible and useful result.

Claim Rejection – 35 USC §112

Referring now to paragraph 7 of the Official Action, claims 25-27 are rejected under 35 USC §112, first paragraph as failing to comply with the enablement requirement and specifically directed to a single means claim and therefore subject to an undue breadth rejection in view of *in re Hyatt*. Claims 25-27 have been amended in a manner to make these claims independent and to recite that the claimed device has been configured to perform a plurality of operations. It is clear from the specification and drawing and in particular, the description of the master device (delagator) (11), server (12) and slave device (delagatee) (13) that each of these devices performs these operations and that messages are transmitted and received as clearly shown in Figures 1-3 and the accompanying description at page 11, lines 13 through page 26, line 24.

It is specifically noted at page 26, lines 17-24 that the master device, slave devices and server each comprise a processing component for performing the processing described for the respective unit, as well as a storage component for storing all of the values required at the respective unit for the described processing, as well as a communication component for performing the described exchange of data with a respective other unit. As a result, claims 25-27 as amended are believed to meet the enablement requirement of 35 USC §112, first paragraph since the claimed configuring of the respective devices is fully disclosed in the drawings and specification.

Referring now to paragraphs 8 and 9 of the Official Action, claims 1-27 are rejected under 35 USC §112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter that applicant regards as the invention and specifically the assertion that "splitting" a key into two parts is indefinite. In response thereto, the previously recited "splitting the master key into a first part and a second part" as set forth in original claim 1 for example, has been

amended to recite "generating a first part and second part of a predetermined secret master key, said predetermined secret master key being available at said master device and said first part and said second part being combinable to said secret master key". It is believed that this recitation is definite and supported by the specification, including page 13, lines 4-17 which describe generating a first part d_1 based on a random number and then obtaining the second part from the available master key d based on the equation $d_2=d-d_1$. Furthermore, the claimed forwarding of a piece of information enabling the slave device to perform a partial secret key operation based on the first part (d_1) of the secret key is definite and disclosed in the specification, including page 14, line 5 through page 15, line 11 which describe that a random number v is transmitted from the master device to the slave device in message II and that the received value v allows the slave device to compute half-key d_1. In addition, the claimed forwarding of the second part (d_2) of the secret key is definite and disclosed in the specification, including page 15, lines 13-20 which indicates that the second half-key d_2 is provided from the master device to the server in message III.

Referring now to paragraph 10 of the Official Action, claims 1-27 are rejected because the preamble of claim 1 does not support the body of the claims. Claim 1 has been amended to cancel the preamble as previously recited. Furthermore, the body of amended claim 1 clearly sets forth the actions for sharing an authorization. It is clear that providing a device with the authorization to use specific resources requires that this device be enabled to use these resources. Having the authorization to use specific resources does not necessarily imply that this authorization is actually used at any particular time. For example, in another context, a person could be registered for online banking and therefore be authorized to access an account over the Internet even if such a person does not make use of that authorization.

Specifically, with regard to amended claim 1, a method is claimed in which at first only a master device (delagator) is authorized and thus able to use certain resources, as it is in possession of a secret master key, which is required to access these resources. The claimed master device then shares its authorization to enable

an additional device (slave device acting as a delagatee) to use the resources. In addition, a server also is forwarded a second part of a secret master key for enabling the server to perform a partial secret key operation on messages received from the slave device and thus the slave device and server have access to a respective partial master key, which would be combinable to the original master key, and the slave device is now enabled and thus authorized in cooperation with the server to use the resources. Thus, it is respectfully submitted that claim 1 as amended does provide for the slave device in cooperation with the server to be enabled and thus authorized to use the recited resources.

It is therefore believed that claims 1-27 as amended are definite and enabled.

In this regard, it should be noted that newly submitted claims 28 and 29 are independent method claims for a slave device and/or a server and for reasons corresponding to those presented above with respect to claim 1, are both enabled by the specification and drawings of the application and are definite and therefore in compliance with 35 USC §112, first and second paragraphs.

Furthermore, newly submitted claims 30 and 31 correspond to amended claims 25 and 26, but are written in means plus function format, and therefore are also believed to be supported by the original application as filed and in compliance with 35 USC §112.

Claim Rejections – 35 USC §103

Referring now to paragraph 11 of the Official Action, claims 1, 12-19 and 25-26 are rejected under 35 USC §103(a) as unpatentable over applicant's admitted prior art (APA) further in view of Stallings (William Stallings, "Cryptography and Network Security", second edition, 1998, ISBN: 0138690170). It is asserted that the APA discloses splitting a secret master key at a master device into a first part and a second part, wherein the master device is acting as a delagator of the authorization; forwarding a piece of information to a slave device acting as a delagatee of the authorization, which piece of information enables the slave device to perform a partial secret key operation on messages based on the first part of the secret master

key; and using the second part of the secret master key to enable the master device to perform a partial secret key operation on messages received from the slave device based on said second part of said secret master key (relying on APA). It is asserted that the APA does not disclose forwarding the second part of the secret master key to a server and Stallings is relied upon for forwarding the second part of the secret master key to a server.

The Claimed Invention

In terms of claim 1, the invention is directed to a method comprising the following actions:

A Generating at a master device a first part and a second part of a predetermined secret master key, said predetermined secret master key being available at said master device and said first part and said second part being combinable to said secret master key, wherein resources are accessible via messages on which a secret key operation was applied with said secret master key and wherein said master device is acting as a delagator of an authorization to use said specific resources.

B Forwarding said first part to a slave device acting as a delagatee of said authorization, which first part enables said slave device to perform a partial secret key operation on messages based on said first part of said secret master key.

C Forwarding said second part of said secret master key to a server for enabling said server to perform a partial secret key operation on messages received from said slave device based on said second part of said secret master key.

In view of these actions, it is noted that an object of the invention is to provide an improved method for sharing the authorization to use specific resources among

multiple devices (see page 4, line 27 through page 5, line 7). The actions recited in claim 1 as summarized above provide the advantage that resources may be used via several devices and by different users concurrently (see page 4, lines 14-20).

Prior Art

The Office refers to the APA and to Stallings (noted above), as well as MacKenzie (MacKenzie and Reiter, "Delegation of Cryptographic Servers for Capture – Resilient Devices", Proceedings of the 8th ACM Conference on Computer and Communications Security, pages 10-19, ISBN: 1-58113-385-5, 2001).

Networked cryptographic devices resilient to capture (MacKenzie et al.)

This document had been acknowledge in the background section of the present application (APA).

A device performs each signature or decryption operation individually by interacting with a server. When the device is initialized, two shares of the device's private key are generated. The first share is constructed so that it can be generated from the user's password and information stored on the device. The second share, plus other data for authenticating requests from the device, are encrypted under a public key of the server to form the device's ticket. Both shares are then deleted from the device.

In the device's signature or decryption protocol, the device sends its ticket plus evidence that it was given the users password. The server verifies this using information in the ticket, and then the server contributes its portion of the computation using its share. Together with the device's contribution using its share (generated from the user's password) the signature or decryption can be formed. (chapter 5, page 17, left column, first paragraph).

Cryptography and network security (W. Stallings)

To achieve a stronger security for public-key distribution in a private-key/public-key encryption model, a tighter control over the distribution of public keys from a directory is described. A central authority maintains a dynamic directory of public keys of all participants. In addition, each participant reliably knows a public key for the authority.

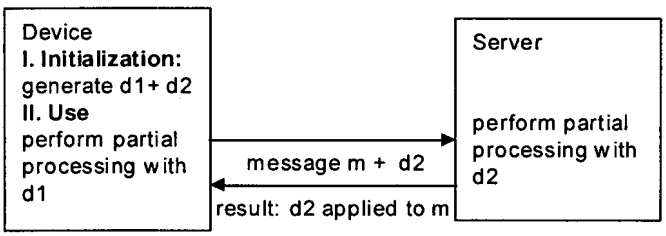
Upon request by device A, the authority transmits to A a message encrypted with the authority's private key, the message including the public key of device B (which A can use to encrypt messages destined for B). Device B may retrieve A's public key from the authority in the same manner. (Public-Key Authority, pages 184-185).

Non-obviousness

Claim 1

As stated above, the Office asserts that claim 1 as originally presented is obvious in view of the APA, including the disclosure by MacKenzie as mentioned in the application and in addition, the Stallings reference.

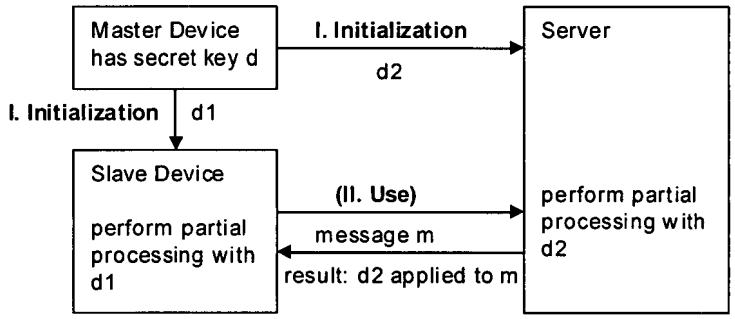
The MacKenzie reference deals exclusively with a basic server-aided secret key operation, in which a device splits a key, keeps information on one part of the key itself and provides information on the other part of the key to the server when a secret key operation is to be performed. The approach is summarized in the following figure:



This is an approach from which the present application proceeds, as explained in the Background of the Invention section.

When proceeding from the MacKenzie reference, a problem to be solved remains; specifically, how to enable a sharing of an authorization to use specific resources among multiple devices. That is, one (master) device has such an authorization and another (slave) device is to be enabled to make use of the authorization as well.

This problem is solved according to amended claim 1 in that a device which is in possession of a secret key enabling a use of specific resources generates two parts of this secret key (action A) and provides information on one part to a slave device (action B) and the other part to a server (action C). The slave device is thereby enabled to perform a server-aided secret key operation independently of the master device (action C). The approach is illustrated in the following figure:



The MacKenzie reference deals with networked cryptography, as does claim 1. MacKenzie however is not related to sharing the authorization to use specific resources among multiple devices. Rather, it deals only with one device and a server. Thus, the method described in the MacKenzie reference differs *per se* from the method of claim 1.

During an initialization, the device of the MacKenzie reference generates a first part and a second part of an available secret key. Thus, action A of claim 1 might be considered to be known from the MacKenzie reference, except for the

device acting as a delagator.

The device of the MacKenzie reference does not forward a piece of information relating to the first part of the master key (d1) to another (slave) device, though. Rather, during a later use case, the device may provide the information relating to the second part of the master key (d2) together with a message to which a secret key operation is to be applied to a server. Thus, action B of claim 1 is not disclosed in the MacKenzie reference.

The device of the MacKenzie reference does forward a piece of information relating to the second part of the master key (d2) to a server during a later use case, but for enabling the server to apply a secret key operation based on the second part to a message equally provided by the same device. It does not forward a piece of information relating to the second part which enables the server to perform a partial secret key operation on messages received from a second (slave) device. Thus, action C of claim 1 is not known exactly from the MacKenzie reference either.

On the whole, it becomes apparent that since multiple devices are obviously not dealt with at all in the MacKenzie reference, this document (or the related acknowledged prior art) is not suited to provide any suggestion at a solution for sharing an authorization among two devices. The MacKenzie reference does not relate to sharing an authority but to ensuring that an authority can only be used in common by a device and a server for reasons of security.

The missing information - namely providing one part of a secret key to a slave device and another part of the secret key to a server for delegating an authority to use certain resources to the slave device - can also not be found in the Stalling reference.

The Stalling reference only discloses providing a *public key* to a server and not a *part of a secret key*. Further, the Stalling reference does not propose any transmission of information relating to a *secret key part* on the one hand to a server and on the other hand to *another device* either. Further, the Stalling reference does not relate to the sharing or delegating of authorization. It just makes sure that a public key belongs to a device from which it is pretended to belong.

In summary, none of the cited references discloses that a master device generates a first part and a second part of a secret key and provides information on *one part to a server and the other part to a slave device* for use in a secret key operation. Thus, it is respectfully submitted that claim 1 as amended is not suggested by the APA in view of Stallings.

Since claim 1 is believed to be distinguished over the cited art, it is respectfully submitted that claims 2-24, all of which ultimately depend from claim 1 are further distinguished over the cited art as cited at paragraphs 11-19 of the Official Action.

Claims 25, 26 and 27 are respectively directed to a delagator/delagatee and server configured for performing the actions recited in amended claim 1 and for similar reasons, are believed to be distinguished over the cited art.

Newly submitted independent method claims 28 and 29 respectively recite the actions from the perspective of a slave device and/or a server as recited in claim 1 and for similar reasons, are believed to be distinguished over the cited art.

Newly submitted independent apparatus claims 30 and 31 correspond to the amended delagator and delagatee independent claims 25 and 26 but are written in means plus function format and for similar reasons, are believed to be distinguished over the cited art.

In view of the foregoing, it is respectfully submitted that the present application as amended is in condition for allowance and such action is earnestly solicited.

Respectfully submitted,

Dated: April 23, 2007

Alfred A. Fressola
Attorney for Applicant
Reg. No. 27,550

WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
Bradford Green, Building Five
755 Main Street, P.O. Box 224
Monroe, CT 06468
Telephone: (203) 261-1234
Facsimile: (203) 261-5676
USPTO Customer No. 004955